## REMARKS

To accelerate prosecution, claims 8-40 have been canceled, and the applicant reserves the ability to pursue claims directed to similar subject matter in a continuing application.

The application now includes claims 51-53.

The office action summary references claims 51-53; however, the office action text only refers to claims 51-52. For purposes of timely responding, the undersigned has treated the office action as if claims 51-53 were rejected as being drawn to non-statutory subject matter under 35 U.S.C. 101 and as being anticipated by U.S. Patent 6,206,829 to Iliff under 35 U.S.C. 102. Both rejections are traversed.

The application describes a computerized methodology which allows personal information (e.g., clinical data) to be used by a web site operator to enhance an anonymous user's use of the web site while maintaining the security and confidentiality of the personal information (e.g.., the web site operator does not have information which would link the personal information to a particular person). In particular, the web site operator would have the web pages of the web site indexed by industry standard medical codes (see page 6 of the application et seq.). The web site would include a user record for each user which also include the industry standard medical codes (see page 7). Thus, the user, when visiting the web site, might be presented with web pages that are paired to his or her medical codes, or his or her searches might be automatically modified to identify web pages which relate to his or her medical history (as defined by the codes), or his or her searches may be modified based on the statistical browsing habits of other user's with similar codes, or by a variety of other mechanisms (see pages 7-8, 24-29, and Figure 7-9 of the application).

Because one aspect of the invention allows for person specific data to be used at a web site, there invention includes specific mechanism for maintaining the security of the person specific data. For example, the claimed methods assure that the person specific data will not be compromised by the web site operator (or a person that compromises the security of the web site), and individuals that use the web site cannot learn private information about other individuals.

**35 U.S.C. 101**

Contrary to the assertions made in the office action, claims 51-53 are not "software per se". Rather, the claimed inventions provide a concrete, tangible result, and require the use of computer hardware or firmware.

With respect to claim 51, and, by example, Figures 2 and 4 of the application, it can be seen that a web server 54 and a registration authority server 82 are used in the practice of the invention. As explained on pages 11, line 19 to page12, line 18, the web server is a computer that provides world wide web services on the internet, and can take a variety of different forms. The registration authority server 82 can also take a number of different forms, and serves the function of creating and assigning each user a unique anonymous identifier (UAI) (see page 14, at line 19). As explained on pages 14 and 15 of the application, once a UAI is assigned to a user, it never changes; therefore, a user may migrate to other health plans without interruption of service on the web site since the UAI is generated by the registration authority, not the health plan.

Thus, with respect to claim 51, it can be seen that the computer systems of three different entities are involved in order to allow a user to securely benefit from enhanced browsing on a web site in a secure fashion. In the Example in the application, there are computers at the health plan, computers at the web site operator, and computers at the third party registry authority. Claim 51 has been amended to highly these elements. Further, Claim 51 describes and recites steps for a process whereby the personal information of a plurality of users is made accessible for use without compromising the personal information. Specifically, and by example with reference to Figure 3, a health plan which is the repository of personal information and clinical data sends only the personal information to the registration authority and send de-identified data to the web site operator for use with the web server. The health plan provides these two types of information to different databases on different servers controlled by different people with surrogate IDs. The registration authority 82 generates a UAI for each user, and sends surrogate ID/encrypted UAI mapping information to the Web site operator (not the health plan). Note that, the result is that the health plan cannot monitor a person's use of the web site (unless there some provision between the user and the health plan) because they do not have the UAI/surrgate ID mapping, the web site

operator cannot identify a particular person that is using the web site (because they only possess the UAI) but can offer that person enhanced browsing capabilities which uses his or her personal (e.g., clinical information), and the trusted registry authority has no access to the clinical information. Thus, the process provides for the secure transfer of personal information that enables that information to be used without compromising a persons personal information.

Similarly, claim 52 recites the use of a registration authority server, a web server, and a certificate authority server (see 92 in Figure 4—as explained on page 19, the certificate authority server generates a user certificate that includes an encrypted form of user's password). The subject matter of claim 52 is directed to a process which allows a user to be authenticated at a WWW site residing on a web server in a highly secure fashion. As discussed above, claim 51 the true identify of a user is verified at a registration authority server, not the web server which will be accessed by the user. Rather, at the web server, the user is anonymous; however, because the web server is provided with surrugate ID/UAI mapping, a web ID is created at the web server. A certificate authority server creates a password for use by the user. With reference to Figure 5 of the application, it can be seen that when a user wants to use the web site, he or she uses their computer to supply a web ID to the web server. If the web ID exists, the web server will prompt the user for a password. The password provided will then be authenticated at the certificate authority. The process, as claimed in claim 52, assures that the only party that know the true identity, web ID, and password of the user is the user. Thus, the method provides a process which will enable user to securely use (anonymously) a web site which has enhanced browsing features that benefit the anonymous user that stem from his or her personal data being employed by the web site operator (without the web site operator knowing the user). Claim 53 depends on claim 52 and also specifically recites the use of servers in the authentication process.

**35 U.S.C. 102**

The Iliff patent is drawn to a system which purportedly generates person specific medical advice. This advice can be rendered over the telephone or via the internet (Figures 24 and 25).

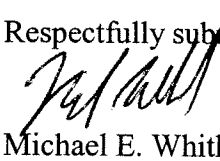
Figure 24 of Iliff aptly illustrates that all of the features of the claimed invention of the present application are wholly lacking in Iliff. On page 7 of the office action, it appears that the Examiner has equated simplistic password login protections with the claimed invention. Note from Figure 24 referenced by the Examiner on page 3 of the office action, the user 2116 is connected through the internet 2102 to the MDATA computer 2108. The MDATA computer 2108 includes the patients identification and medical history information (see Figures 5a-g and 6–see also column 7, line 1 et seq. where it is clear that what the MDATA computer does is provide a diagnosis and or advice to a KNOWN patient. This is particularly highlighted in column 13 of Iliff where it is explained that the advice is patient specific and that different patients may get different advice when they provide the same symptom information because they have different patient histories. With due respect to the Examiner, all that is shown in the passages identified in Iliff (column 35, lines 4-61; column 69, lines 15-61; and column 74, lines 38-65) are remote login procedures, the ability to provide data remotely, and provisioning of PIN numbers. In no way does Illiff show or suggest processes that utilize of a web server and registration server with indexing of de-identified personal information by an anonymous ID (as required in claim 51), or processes that use a web server, registration server, and a certificate authority server in a manner that assures only the user has knowledge of his true identity, web ID, and password (as required by claim 52).

In view of the foregoing, it is respectfully requested that the application be reconsidered, that claims 51-53 be allowed, and that the application be passed to issue.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic or personal interview.

A provisional petition is hereby made for any extension of time necessary for the continued pendency during the life of this application. Please charge any fees for such provisional petition and any deficiencies in fees and credit any overpayment of fees to Attorney's Deposit Account No. 50-2041.

Respectfully submitted,



Michael E. Whitham
Reg. No. 32,635

Whitham, Curtis, Christofferson & Cook, P.C.
11491 Sunset Hills Road, Suite 340
Reston, VA 20190

Tel. (703) 787-9400
Fax. (703) 787-7557

Customer No.: 30743